Commander, Navy Installations Command

CAC PIN Reset
User's Manual
And
Business Policy

November 2008

Version 2.1.0.2.3

1. INTRODUCTION 1
1.1. PURPOSE AND SCOPE 1
1.2. BACKGROUND 1
1.3. CPR WORKSTATION (CPR-WS) DESCRIPTION 2
1.4. ROLES AND RESPONSIBILITIES 3
1.4.1 Defense Manpower Data Center (DMDC) 3
1.4.2 CNIC CAC Program Management Office (PMO) 3
1.4.3 Trusted Agent Security Manager (TASM) 3
1.4.4 CAC PIN Reset Trusted Agent (CTA) 4
1.4.5 Help Desk Support 5
1.5. POLICY & USER'S MANUAL MAINTENANCE 5
2. GENERAL PROVISIONS 5
2.1. INTERPRETATION AND ENFORCEMENT 5
2.1.1 Severance of Provisions, Survival, Merger, and Notice 5
2.1.2 Dispute Resolution Procedures 5
2.2. PUBLICATION AND REPOSITORY 6
2.2.1 Publication of POC, TASM, and CTA Information 6
2.2.2 Frequency of Publication 6
2.2.3 Access Controls 6
2.2.4 Repositories 6
3. REGISTRATION AND MANAGEMENT OF USERS 6
3.1. TASM REGISTRATION 6
3.2. TASM REVOCATION 7
3.3. TASM INFORMATION UPDATE 7
3.4. CTA REGISTRATION, REVOCATION, AND INFORMATION UPDATE 8
4. TRAINING 8
4.1. TRAINING MATERIAL AVAILABILITY 8
4.2. TASM TRAINING 8
4.3. CTA TRAINING 8
4.4. ACKNOWLEDGMENT OF RESPONSIBILITIES 8
5. PERFORMING THE SITE SURVEY 9
6. EQUIPMENT ASSEMBLY AND SHIPMENT 9

6.1. BUILDING THE CPR WORKSTATION 9
6.2. SHIPPING THE CPR WORKSTATION 10
6.3. PROPERTY ACCOUNTABILITY 10
7. REQUESTING NEW OR ADDITIONAL WORKSTATIONS 10
7.1. NEW CPR CAPABILITY 10
7.2. ADDITIONAL CPR CAPABILITY 11
8. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS 11
8.1. PHYSICAL CONTROLS 11
8.1.1 Physical Access 12
8.1.2 Power and Air Conditioning 12
8.1.3 Water Exposures 12
8.1.4 Fire Prevention and Protection 12
8.1.5 Media Storage 12
8.1.6 Waste Disposal 12
8.1.7 Emergency Actions 13
8.2. PROCEDURAL CONTROLS 13
8.2.1 Trusted Roles 13
8.2.2 Activation Data Protection 13
8.2.3 CPR Workstation Administration 13
8.3. PERSONNEL CONTROLS 13
8.3.1 Background, Qualifications, Experience, and Clearance Requirements 13
8.3.2 Project Officer 13
8.3.3 TASM 14
8.3.4 CTA 14
8.3.5 Background Check Procedures 14
9. TECHNICAL PROCEDURES 15
10. REGISTERING CAC PKI CERTIFICATES 16
11. CTA REGISTRATION 17
12. ADD A USER ACCOUNT TO THE WORKSTATION 17
13. APPLICATION LOGON 19
14. RE-SETTING A CUSTOMER'S PIN 21
15. TECHNICAL ASSISTANCE 22

15.1. TROUBLESHOOTING PROCEDURES 22

15.1.1 Web Based Information 25

15.2. HELP DESK SUPPORT 25

15.2.1 CPR-MS Information Availability 26

16. USER INFORMATION UPDATES 26

17. CPR SITE ROSTER VIEWING... 28

18. USER REVOCATION 29

19. AUDIT FILE REQUESTS 29

19.1. REPORTING REQUIREMENTS 29

19.2. PROTECTION OF AUDIT FILES... 29

19.3. REQUEST FOR AUDIT FILES... 29

19.4. FREQUENCY OF SUBMISSION.. 30

20. AUDIT FILE RETRIEVAL 30

21. POINTS OF CONTACT.. 30

1. INTRODUCTION

1.1. Purpose and Scope

The Common Access Card (CAC) Personal Identification Number (PIN) Reset system (hereafter referred to as CPR) was developed to provide a portable, flexible, single purpose system, capable of providing timely PIN reset capability to the field in a myriad of operating environments. The system was designed to securely solve the PIN reset problem, using Commercial off the Shelf (COTS) hardware over a non-NMCI network.

This document describes the business policies and step by step directions for CPR users to employ when operating CPR equipment. It should be read by all potential Trusted Agent Security Managers (TASMs) and CPR Trusted Agents (CTAs) and consulted for all day to day CPR operations. It will provide detailed instructions to users on the proper procedures to follow for compliance with Navy policy.

1.2. Background

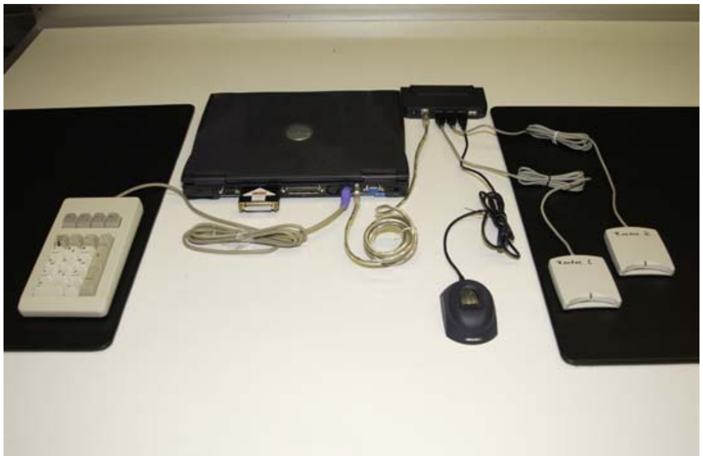
The Real-time Automated Personnel Identification System (RAPIDS) was established in 1981 to provide a secure, automated method of producing identification (ID) cards. In 2000, RAPIDS was upgraded to support the issuance and update of the Department of Defense (DOD) Common Access Card (CAC). The CAC is an ID card with an integrated circuit chip for processing and storing information. The initial issuance of the CAC is achieved through Defense Enrollment Eligibility Reporting System (DEERS)/RAPIDS workstations under the control of Verifying Officials (VOs).

The CAC has a PIN, which is known only to the cardholder. It is 6-8 numeric digits in length that the user enters at issuance. To use any of the certificates or applets on the card, the cardholder must supply the PIN. When a CAC is inserted into a reader, the middleware on the workstation tries to access an applet on the card. The card's response is to ask the user for a PIN. When a PIN is entered, it is sent to the card and validated against the PIN stored on the chip. If the PIN is correct, the card is available for use. A cardholder has 3 attempts to provide the correct PIN. After the third unsuccessful attempt, the PIN management applet in the card "locks" the CAC making it impossible to obtain the certificates or data on the card.

Due to inherent programmatic delays between the issuance of the CAC to users and the fielding of card reader and middleware components to the desktop environment, in many cases the PIN is forgotten by the user, resulting in numerous "locked" CACs. To recover use of the card, users would need to journey to a RAPIDS issuance facility, wait for availability of the DEERS/RAPIDS workstation and have the PIN reset. This results in both a loss of work productivity for the user and diversion of RAPIDS personnel and resources from the primary mission, card issuance. Additionally, RAPIDS issuance facilities are not staffed to provide 24-7 support, making timely PIN reset improbable. The CPR system was developed as a low cost, mobile solution to the problem of "locked" CACs.

1.3. CPR Workstation (CPR-WS) Description

The CPR-WS is a client workstation that provides authentication and secure communications for CPR users and cardholders in support of PIN reset. It is with this component of CPR that TASMs and CTAs have hands-on access to the CPR system.



Component	Description
(1) Computer	Dell Latitude D630, English (220-9540) or equivalent (2.0 GHz, Intel Pentium M Processor, 1.0 GB RAM, 24X CD-ROM, with USB, Parallel, and Serial connectors) (Equivalent systems must be tested and approved by the Defense Manpower Data Center (DMDC))
(2) Smart card encoder/readers	SCM SCR331 USB, external International Standards Organization (ISO) 7816 Class A and AB-compatible, EMV Level 1 and ActivCard USB Reader V2.0
(1) Fingerprint scanner	Identix DFR 2080 USB models
(1) PIN entry pad	Targus PAUK10 USB numeric key pin pad
(1) USB HUB port device	Belkin Hi-Speed USB 2.0 4-port hub (Belkin P/N: F5U224)
(1) Cat 5 RJ45 patch cable	12 Feet
(1) Surge suppressor	Belkin F5C695-TEL for (110Vsites) or ISOBAR EURO-4 (220V sites)
(1) Mouse	Logitech MX310

Table 1. CPR Workstation Hardware Requirements

The workstation uses the Windows XP operating system as a platform for operation of the CPR application. This application, in conjunction with various drivers, applications and middleware for the peripheral equipment, operates to permit controlled access to the DEERS/RAPIDS CPR infrastructure. Authentication of users, the PIN reset process, and limited user management is enabled by this interface. Specific software requirements are detailed in Table 2.

In order to ensure a secure operating environment and guard against unauthorized use, the workstation is locked down and configured specifically for each CPR site. For these reasons, CPR workstations will only function for the specific locations and for the specific users assigned to that site.

The CPR Project Manager from the CAC Program Management Office (CAC PMO) performs the configuration of all CPR workstations owned by the CAC PMO.

Description
MS Internet Explorer version 6.0, SP2 with the Cumulative Security Patch and Secure Socket Layer (SSL) software (via Microsoft's Secure Channel API)
Anti-Virus software for Windows XP and latest Anti-Virus definitions
ActivClient for CAC – PKI Only 6.0 - Windows version
CPR v 2.1.0.2.3 application
SCM SCR331card reader, Identix DFR-2080 scanner and Belkin USB hub drivers
Identicator/Identix quality control and verification software and hard lock driver (Bio Engine SDK 3.0)

Table 2. CPR Workstation Software Requirements

1.4. Roles and Responsibilities

1.4.1 Defense Manpower Data Center (DMDC)

The DMDC (as the DEERS/RAPIDS administrator) is chartered with maintaining and overseeing efficient operation of the CPR infrastructure.

1.4.2 CNIC CAC Program Management Office (PMO)

Commander, Navy Installations Command CAC PMO, is the Navy's focal point for day to day management of the CPR system. Responsibilities include coordination with the Defense Manpower Data Center (DMDC) on matters pertaining to the establishment of CPR sites and requisite equipment build, shipment and follow-on support, oversight of TASM registration, administrative oversight of all CPR users (including CTAs), administration of the CPR Management Service (CPR-MS) and promulgation of CPR training materials.

All matters relating to CPR registration (including sites and users) should be coordinated with the CPR Project Manager located in the CAC PMO (CPR Project Manager: (850)452-7895).

1.4.3 Trusted Agent Security Manager (TASM)

TASMs have the responsibilities of user management, workstation maintenance and administration, equipment storage and accountability in their specific area. Each site is allowed two TASMs, a primary and an alternate.

Specifically, TASMs shall:

- Perform Site ID Surveys, used for CPR Workstation configuration for their specific site.
- Manage all users (TASMs and CTAs) for the CPR Workstations under their control.
- Adhere to all security requirements with regard to the CPR workstation to include installing critical IAVA patches as required and access to CPR equipment.
- Provide local visibility for the CPR program at their site. This may be accomplished via Plan of the Week/Day notes, a newsletter or website, or whatever other means is appropriate for the location. Information should include the location of the CPR capability, hours of operation, phone numbers, and other pertinent data.
- Submit requests for new or additional CPR capability at their site.
- Coordinate all CPR matters with the CPR Project Manager.
- Train an alternate TASM and all CTAs operating CPR equipment within their site.
- Coordinate the repair and/or replacement of CPR equipment under their control.
- Secure and retain property accountability of all CPR equipment under their control.
- Immediately notify the CPR Project Manager if there is a loss of CPR capability at the site.
- Perform CAC PIN Resets.
- At the direction of CPR Project Manager, periodically transmit audit files created on the CPR Workstation for sampling and measurement purposes.
- Ensure positive identification of all CTAs for their site.
- Ensure positive identification of all subscribers requesting CPR.
- Protect access to PINs, including their own, CTAs, and subscribers during the reset process.
- Refer subscribers to their CAC issuance facility when either:
    a. Authentication cannot be positively confirmed

    b. When the PIN cannot be reset (due to non-technical reasons)
- Immediately notify CPR Project Manager if there is any suspected or known compromise of the CPR system.

1.4.4 CAC PIN Reset Trusted Agent (CTA)

The CTAs primary role in the field is to provide CPR. CTAs are registered locally on the CPR workstation by the TASM, using the User Administrator function of the CPR application.

CTAs will:

- Adhere to all security requirements with regard to the CPR workstation and access to CPR equipment.
- Perform CAC PIN Resets.
- Ensure positive identification of all subscribers requesting CAC PIN Resets.

- Secure and retain property accountability of all CPR equipment under their control.
- Immediately notify the site TASM if there is a loss of capability at the site.
- Immediately notify the TASM or CPR Project Manager if there is any suspected or known compromise of the CPR system.
- Protect access to PINs, including their own, and subscribers during the reset process.
- Notify the site TASM of any malfunctions or anomalies with CPR equipment (CTAs should contact CPR Project Manager when the local TASM is unavailable).
- Refer subscribers to their CAC issuance facility when either

  a. Authentication can not be positively confirmed, or

  b. When the PIN cannot be reset (due to non-technical reasons)

1.4.5 Help Desk Support

TASMs and CTAs who are experiencing any difficulty with the CPR process should contact the CNIC Support Center or the CPR Project Manager. This includes workstation configuration, applications, hardware, software, and troubleshooting issues.

CNIC Support Center: (888)264-4255

CPR Project Manager: (850)452-7895

1.5. Policy & User's Manual Maintenance

CNIC CAC Program Management Office (CAC PMO) is responsible for maintaining this Policy & User's Manual. For questions regarding this manual contact the CNIC, CAC Program Management Office, CPR Project Manager, (850) 452-7895.

2. GENERAL PROVISIONS

2.1. Interpretation and Enforcement

2.1.1 Severance of Provisions, Survival, Merger, and Notice

Should any section of this CPR Policy Statement & User's Manual be determined to be incorrect or invalid, all parties including the CAC PMO, TASMs, CTAs, and CAC holders will nevertheless abide by the practices described herein, until provided new policy guidance.

Invalid information in a section or sections of this document does not invalidate other sections. Thus all other sections of this document should be considered otherwise valid.

2.1.2 Dispute Resolution Procedures

The CNIC CAC PMO mediates any policy statement disputes regarding interpretation or applicability.

2.2. Publication and Repository

2.2.1 Publication of POC, TASM, and CTA Information

For the CPR user (TASM and CTA personnel) personal information published in a public location is limited to name, telephone number, email address, and duty location. Under no circumstances is information covered under the Privacy Act of 1974 published in a public directory. This includes information used to populate the CPR-MS for the intent of providing a CPR site locator for the DON community. Although such information may exist in the CPR-MS database, security safeguards isolate this data from public access.

2.2.2 Frequency of Publication

No stipulation.

2.2.3 Access Controls

During CPR:

1. The Windows XP user management security capability and DEERS authentication process controls workstation activity and CPR user access.
2. A biometric verification executes for both the CPR user and CAC holder, and involves two approaches:
    1. A live fingerprint is compared against DEERS database fingerprint information for both the CPR user and CAC holder. If either verification fails, CPR is not a viable option.
    2. A photographic comparison is conducted for the CAC holder.

2.2.4 Repositories

The DEERS records all CPR user registrations and PIN reset attempts, and later transmits this information to the CPR Project Manager for CPR-MS inclusion. Local audit files, also created and saved on the CPR workstation, store more detailed information on CPR users and transactions than that stored in the DEERS. These files are sent to the CPR Project Manager on an as-needed/requested basis. Data is protected during all facets of storage and transmission.

3. <u>REGISTRATION AND MANAGEMENT OF USERS</u>

3.1. TASM Registration

All TASM registrations must be accomplished through the DEERS Security Team via the CPR Project Manager. This is accomplished as follows:

a. An individual who meets the qualifications is nominated by completing a TASM registration request (Appendix C) and a CPR User Qualifications Affidavit (Appendix D) and is forwarded to the CPR Project Manager via mail, fax, in person, or digitally signed email.

b. If the correct format and minimum requirements are met, the CPR Project Manager forwards the TASM request to the DEERS Security Team (DST) for upload into the

DEERS system. Incomplete TASM registration requests or qualification affidavits will be returned.

c. The DST enters the information into DEERS for the new TASM. Once completed, the DST sends confirmation of the upload to the CPR Project Manager.

d. The CPR Project Manager notifies the new TASM of registration in DEERS via digitally signed email. Additionally, the CPR Project Manager inputs the TASM's contact information into the CPR Management Service.

This can take up to 48 hours due to DEERS processing time. If the new registration is for a primary TASM, this confirmation may be further delayed until the CPR workstation is received at that site. The only positive way to ensure that the TASM has been successfully registered is to attempt authentication to the DEERS system via the CPR workstation.

In the event that the TASM cannot successfully log on to the CPR workstation after 48 hours he/she should contact the CPR Project Manager immediately to correct the problem. The CPR Project Manager will coordinate with the DST office to re-accomplish registration.

3.2. TASM Revocation

TASM CPR privileges will be revoked under any of the following conditions:

- Under investigation (or have been convicted) of any offense punishable by the Uniformed Code of Military Justice (UCMJ) or equivalent civilian law
- Relieved of duty
- Left military service or otherwise became disassociated with the U.S. Navy
- Transferred out of the command

All TASM revocations must be through the DEERS Security Team via the CAC PMO. This is accomplished by notifying the CPR Project Manager of the requirement to revoke a TASM and submitting a Request for TASM Revocation form (Appendix C) via mail, fax, in person, or digitally signed email.

a. If the submission is in the correct format, the CPR Project Manager forwards the TASM Revocation Request to the DEERS Security Team (DST) for upload into the DEERS system.

b. The DST enters the revocation request into DEERS for the TASM to remove him/her from the CPR sign-on table. Once completed, the DST sends confirmation of the revocation to the CPR Project Manager.

c. The CPR Project Manager notifies the command of the completed revocation via digitally signed e-mail. Additionally, the CPR Project Manager removes the TASM's contact information from the CPR Management Service and archives the TASM records.

3.3. TASM Information Update

From time to time, it may be necessary to update TASM contact information such as e-mail address, phone number(s), fax number(s), etc. This must be accomplished through the DEERS Security Team via the CPR Project Manager as follows:

a. A completed TASM Information Change Request (Appendix G) is submitted along with the reason, to the CPR Project Manager via mail, fax, in person, or digitally signed email.

b. In the event the TASM Information Change Request is incomplete, the CPR Project Manager will return the form.

3.4. CTA Registration, Revocation, and Information Update

All registrations, revocations, and information updates are accomplished locally by the TASM. The TASM must register the CTA via the Security Online Web Application and create a user account on the CPR workstation. See Sections 11 & 12 for step by step instructions.

4. TRAINING

4.1. Training Material Availability

The CAC PMO distributes approved CPR training materials. This is provided in person, via CD-ROM (mailed via the postal system or recognized delivery service), email, or accessed online at http://pmo.cac.navy.mil .

4.2. TASM Training

The CPR Project Manager is the point of contact for TASM training.

Training is initiated when an individual is identified as a TASM and registration has been accomplished. TASM training is self-directed training using materials provided by the CAC PMO. Alternate TASMs should be trained by the primary TASM.

4.3. CTA Training

Because of the limited responsibilities associated with the CTA privileges, all CTA training is conducted hands-on locally by the TASM. This is performed according to training materials provided by the CAC PMO.

Training is initiated when the CTA is identified to the TASM and registration has been accomplished.

The TASM conducts training with the new CTA, to include workstation logon, application logon, PIN reset, workstation sign-out procedures (to be determined locally) and security requirements. TASMs shall ensure that each CTA candidate fully understands each of these processes prior to completion of the training. This may be accomplished via any means the TASM deems necessary, to include locally administered tests.

4.4. Acknowledgment of Responsibilities

All TASMs and CTAs receiving CPR user training must complete and sign an Acknowledgement of Responsibilities Form. By completing this form (see Appendixes E & F), TASMs and CTAs acknowledge that they have received CPR training and that they understand their obligations as specified in this policy statement. The form must be completed in the presence of a person who verifies the user’s identity and also signs the form.

A copy of the TASM/CTA Acknowledgement Form is forwarded to the CPR Project Manager (via mail, fax, in person, or digitally signed email). TASMs should retain a local copy.

Acknowledgement forms completed for CTAs may be signed by the TASM conducting the training. CTAs may retain a copy for their own records.

Consistent with the requirements specified in the RAPIDS Verifying Official Certificate Practice Statement, acknowledgement forms must be retained for a period of 11 years.

For:

1. **TASMs** – The CAC PMO maintains these forms (and may also archive them)
2. **CTAs** – The site TASM maintains these forms until the CTA no longer performs CPR-related site functions. The CAC PMO maintains the CTA Acknowledgement of Responsibilities form (Appendix F).

5. PERFORMING THE SITE SURVEY

Before a CPR workstation is configured and shipped to a new CPR location, completion of a site survey is required. This is necessary to ensure that the new workstation meets all security requirements for the local area network and to set the proper configuration settings. Normally, the primary TASM is in the best position to complete this survey. Local network administrators and security personnel should be consulted when necessary. CPR is not currently NMCI certified.

TASMs will conduct site surveys as follows:

a. The command requests a site survey from the TASM by forwarding the Site Survey Worksheet (Appendix G). A site survey only needs to be accomplished once for a CPR site. Once the site is operational, no additional surveys are required.

b. The TASM completes the worksheet, ensuring all applicable network security settings or circumstances are identified. Local area network administrators and security personnel should be consulted as necessary.

c. Once completed, the TASM returns the worksheet to the CAC PMO via mail, fax, in person, or digitally signed email. Incomplete Site ID Survey worksheet will be returned to the TASM for correction.

d. Upon receipt of the Site ID Survey, the CAC PMO Project Officer reviews it for completeness. If all necessary information is provided, the request is forwarded along with the applicable Site ID and TASM registration information to DMDC.

6. EQUIPMENT ASSEMBLY AND SHIPMENT

This section applies to those sites that are using equipment owned and provided by the CAC Program Management Office.

6.1. Building the CPR Workstation

The following prerequisites apply to building and configuring a CPR workstation:

- Identifying at least one site TASM (the primary TASM)
- Establishing a site ID
- Specifying the local configuration (via completing the Site Survey in Appendix G)

Once these actions are complete and all required data is obtained for a site, the CPR Project Manager shall commence the workstation build.

The CPR Project Manager assembles all hardware, installs software, and configures the workstation for the specific site. The CPR Project Manager then tests and evaluates the workstation for quality control standard compliance, and upon successfully passing evaluation, releases the workstation for shipping. Workstations that do not pass testing are returned for rework.

6.2. Shipping the CPR Workstation

After successful testing, CPR workstations and associated equipment are packaged for shipment. This includes peripherals, additional software applications, and CPR user documentation. Additional documentation includes an inspection checklist and setup procedures. An initial password for the primary TASM is generated and sent (via a separate email). This password must be changed upon the TASM's first CPR workstation login.

Note: Although the password allows limited CPR workstation access, it cannot access further functions without an inserted TASM CAC and valid biometric authentication.

6.3. Property Accountability

The following describes the property accountability process for a CPR workstation shipment.

a. The CPR workstation shipment is accepted by the office representative authorized by the Commanding Officer/Officer in Charge who in turn notifies the site TASM for equipment pickup.

b. The TASM acknowledges receipt and official custody of the CPR workstation(s) via completion and return (to CPR Project Manager) of the accompanying custodial shipping/transfer receipt.

c. The TASM conducts a physical inspection, performs setup procedures, and tests to verify workstation operation. If all inspections, tests, and configuration procedures are successful, the TASM may begin to administer users and/or conduct PIN resets.

Note: If TASM training is conducted via web-based or hard copy materials, the TASM undergoes this training now. The TASM then completes the TASM and CTA Acknowledgement of Responsibilities Form (Appendix E) and returns it to the CAC PMO.

7. REQUESTING NEW OR ADDITIONAL WORKSTATIONS

7.1. New CPR Capability

New CPR requests apply to sites having no CPR capability and it is not included in approved programmed plans. Local authorities (normally the local Commander) establish requirements/requests for new CPR capability. Commands willing to purchase CPR equipment with their own funds should clearly state this in your request.

The following describes the process for requesting new CPR capability.

a. The local authority contacts the CPR Project Manager to initiate an initial capability request. Commanding Officers/Officers in Charge will create their own internal procedures for initiating and reviewing capabilities at the site level.

b. Submit a capability request letter to the CPR Project Manager, via a memorandum signed by the local Commander (or designated representative) at the existing or potential site. This memorandum must include justification for the requirement and specifies whether the equipment is to be funded by the local installation.

c. CAC PMO, after completing the review process, takes one of these actions:
   - Returns the request for additional information
   - Disapproves (returns with rationale)
   - Approves

d. Register a TASM (Section 3).

e. After completion of TASM training (Section 4), perform a site survey (Section 5).

f. Register and train Alt TASM and CTAs as necessary.

7.2. Additional CPR Capability

This request applies to sites already having CPR capability; however local authorities (normally the local Commander or TASM) have determined that an insufficient number of workstations exist. The following describes the process for requesting additional CPR capability.

a. The local authority contacts the CPR Project Manager to initiate an additional capability request. Commanding Officers/Officers in Charge will create their own internal procedures for initiating and reviewing capabilities at the site level.

b. Submit a capability request letter to the CPR Project Manager, via a memorandum signed by the local Commander (or designated representative) at the existing or potential site. This memorandum must include justification for the additional requirement and specifies whether the equipment is to be funded by the local installation.

c. CAC PMO, after completing the review process, takes one of these actions:
   - Returns the request for additional information
   - Disapproves (returns with rationale)
   - Approves

8. <u>PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS</u>

8.1. Physical Controls

When the CPR workstation is in use, an authorized TASM or CTA must always be present. When not in use, the workstation must have all CACs removed from the card readers.

CPR workstations will be protected against theft, loss, and unauthorized use as described in the next section.

8.1.1 Physical Access

TASMs and CTAs will ensure that if the workstation is involved in travel, under no circumstances shall the equipment be left unattended. This includes unattended baggage checking on commercial conveyance (such as an airplane, train, bus or taxi).

The following rules apply to CPR workstation security:

1. An approved TASM or CTA must be present any time the CPR workstation is powered up and in use
2. TASMs and CTAs must ensure that all CACs are removed from the card readers before securing the workstation.
3. Under no circumstances shall TASMs or CTAs share CACs, passwords, or PINs.
4. All Navy-accepted property accountability measures will be taken to ensure that TASMs retain custodial oversight and responsibility for the CPR assets under their control. Because many CPR site users may access this equipment, this rule is particularly important. When other CPR site users sign out equipment, it is the TASM's responsibility to ensure the proper documentation (such as a hand receipt) is completed to identify a chain of custody. Further, when CPR equipment is returned to the TASM, it is jointly the responsibility of the TASM/CTA returning the equipment to inspect the asset(s) for damage and proper operation. In the event of damage, appropriate investigation(s) are initiated.

8.1.2 Power and Air Conditioning

The following hardware requirements relate to CPR workstation power and temperature control:

1. Store the CPR workstation in a dry, preferably temperature-controlled environment
2. Use a surge suppressor when the CPR workstation is in use
3. Batteries for CPR workstation laptops should be charged prior to use and protected from damage or heat

8.1.3 Water Exposures

The CPR workstation shall be located so as to prevent undue exposure to dirt, dust, inadvertent jolting or jarring and water collection/immersion.

8.1.4 Fire Prevention and Protection

Fire extinguishers shall be located in close proximity to CPR assets and associated storage cabinets. The site's disaster recovery plan should include fire disaster recovery procedures.

8.1.5 Media Storage

The CPR workstation requires no anticipated media storage requirements.

8.1.6 Waste Disposal

Normal office waste is periodically removed or destroyed. CPR users will not write down passwords for CPR workstation access. CPR users or CAC holders must not write down their PIN during the reset process, but rather commit the PIN to memory. Any generated paper waste containing sensitive information must be shredded or incinerated immediately following the reset activity.

8.1.7 Emergency Actions

To protect the operational CPR workstation and peripherals from unauthorized use during hostile actions and natural disasters, CPR users must (if they cannot be safely evacuated) physically destroy the CPR equipment or remove and destroy the hard drive.

8.2. Procedural Controls

8.2.1 Trusted Roles

Sections 1.4.3 and 1.4.4 define the TASM and CTA responsibilities. The procedures for exercising these responsibilities are described throughout this policy statement and user's guide.

8.2.2 Activation Data Protection

Because the PIN that activates CAC applications also provides access to a holder's private PKI keys (and consequently can allow someone to assume the holder's identity), it is imperative that only the CAC holder knows this number. PINs must not be shared among CAC holders or with the TASM or CTA during the reset process.

8.2.3 CPR Workstation Administration

To maintain DMDC security for DEERS/RAPIDS system access, all CPR workstations must meet stringent security requirements as stipulated in the System Security Authorization Agreement (SSAA) or the Net Worthiness Certification. Toward that end, CPR workstations assembled by the CPR Project Manager are locked down to prevent access to all but the necessary functions required by TASMs to administer other CPR users and perform the PIN reset process.

8.3. Personnel Controls

8.3.1 Background, Qualifications, Experience, and Clearance Requirements

CPR managers and users must meet the following minimum requirements.

8.3.2 Project Officer

The CPR Project Manager must:

1. Be a DoD uniformed service member, DoD civilian, or contractor working for the Navy
2. Be capable of sending and receiving digitally signed and encrypted email
3. Have a working knowledge of the Navy field support structure, including populations and missions of units and sites
4. Be familiar with Public Key Infrastructure (PKI), the CAC issuance process, and the Navy's CPR process policy
5. Have not been convicted of a felony offense

6. Be a United States citizen or hold an active security clearance and have not knowingly been denied a security clearance or have had a security clearance revoked
7. Be trustworthy
8. Have a minimum of 12 months of retainability

8.3.3 TASM

A Trusted Agent Security Manager must:

1. Be a U.S. Citizen
2. Be a DoD uniformed service member, DoD civilian, or contractor working for the Navy
3. Be appointed in writing by an approving authority
4. Be capable of sending and receiving digitally signed and encrypted email
5. Be a CAC holder
6. Have completed requisite CPR TASM training
7. Have not been convicted of a felony offense
8. Have not knowingly been denied a security clearance or had a security clearance revoked
9. Have an active and current National Agency Check (NAC) background investigation
10. Be trustworthy
11. Be knowledgeable of Navy equipment accountability procedures
12. Have a minimum of 6 months of retainability

8.3.4 CTA

A CAC Trusted Agent must:

1. Be a U.S. Citizen
2. Be a DoD uniformed service member, DoD civilian, or contractor working for the Navy
3. Be appointed in writing by the (or designated representative) responsible for their site
4. Be a CAC holder
5. Have completed hands-on CPR training (administered by the site TASM)
6. Have not been convicted of a felony offense
7. Have not knowingly been denied a security clearance or had a security clearance revoked
8. Be trustworthy

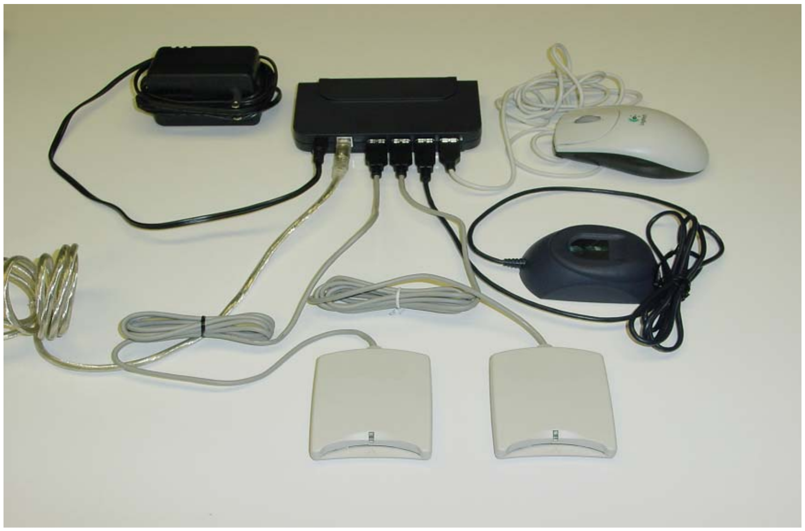
8.3.5 Background Check Procedures

An organization recommending a TASM appointment must submit a CPR User Qualifications Affidavit (Appendix D) with a request for the TASM Registration/Revocation (Appendix C) signed by the Commanding Officer/Officer in Charge (or designated representative). This affidavit states that the recommended TASM meets the requirements of Section 7.3.1 based on the organization’s research, knowledge, and/or interview with the applicant.

9. TECHNICAL PROCEDURES

Workstation Assembly and Setup

1. Plug the *USB 4 Port Hub electrical adapter* into the back of the hub. Connect the *USB Connection Plug* to the adapter port in the USB 4 Port Hub.
2. Connect the opposite end of the *USB connection plug* to the USB port of the Workstation.
3. Connect the *Numeric Keypad* to the Workstation USB port.
4. The peripheral devices should be connected in the following order
    a. ActivCard CAC (CTA) Reader
    b. SCM SCR CAC (User) Reader
    c. Biometric Reader Identix DRF 2080 fingerprint scanner
    d. Mouse
5. With the USB hub port side facing you, beginning from the left side, connect *CAC Readers* in the order above to the first and second port. Connect the *Biometric Fingerprint Reader* to the third port. Connect the *Mouse* to the last port.



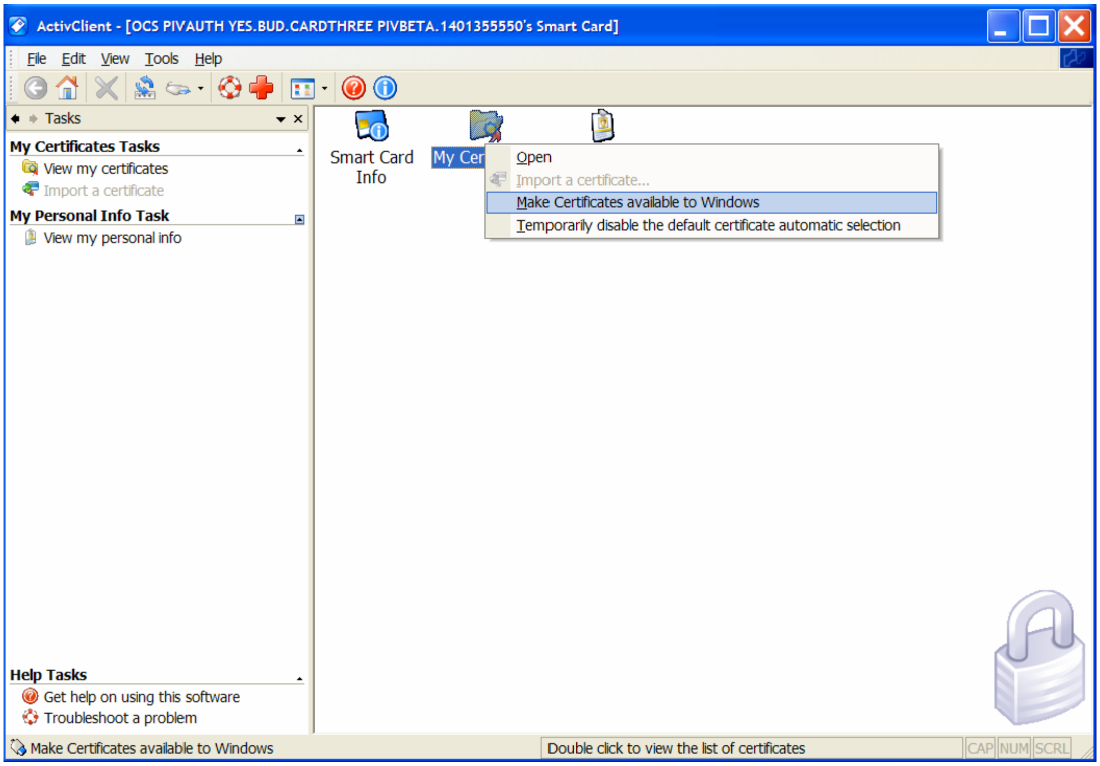
6. To complete workstation assembly, connect the laptop power supply to the laptop. This connection is located on the back of the laptop. Plug the opposite end of the laptop power supply into the surge protector. Plug the surge protector in the wall electricity outlet.
7. Connect the 4 port hub electricity adapter to the surge protector.
8. Connect the laptop to the local non-NMCI network via the ***CAT5 RJ45 network cable***. Plug the opposite end of the local area network cable into the network wall jack.
9. Power on the CPR Workstation. Log in by entering the ***Username*** and ***Password*** provided for you.

Note: Since this is the first login on the CPR workstation, you will be prompted to change the password during login. This will be your **NEW** password and should be used for future logins.

10. REGISTERING CAC PKI CERTIFICATES

1. Double click the ***ActivClient*** icon displayed in the Windows System Tray (this icon will be placed in the tray after installing ***ActivClient*** software) or run the ***ActivClient*** program from the Windows Start/Programs menu.
2. Insert your CAC into the Activcard reader and launch the ***ActivClient*** utility.
3. The ***ActivClient*** window will display.
4. To register certificates, right click on the “My Certificates” icon. From the menu, click on the “Make Certificates Available to Windows” selection.

   Note: All 3 certificates will be registered in this one step.


ActivClient - [OCS PIVAUTH YES.BUD.CARDTHREE PIVBETA.1401355550's Smart Card]
File Edit View Tools Help
Tasks
My Certificates Tasks
View my certificates
Import a certificate
My Personal Info Task
View my personal info
Help Tasks
Get help on using this software
Troubleshoot a problem
Smart Card Info
My Cer
Open
Import a certificate...
Make Certificates available to Windows
Temporarily disable the default certificate automatic selection
Make Certificates available to Windows
Double click to view the list of certificates
CAP NUM SCRL

ActivClient Main Window

5. Click ***OK*** to complete Certificate installation.
6. Your certificates are now successfully registered. Close the ***ActivClient*** window.

   Note: Email certificates are not needed on the CPR Workstation. Perform the following procedures to delete the email certificates from the Certificate store.

7. Double-click the ***Internet Explorer*** icon on the desktop. Once Internet Explorer opens, click ***Tools*** and choose ***Internet Options*** from the menu.

8. Click the ***Content*** tab then click the ***Certificates*** button.

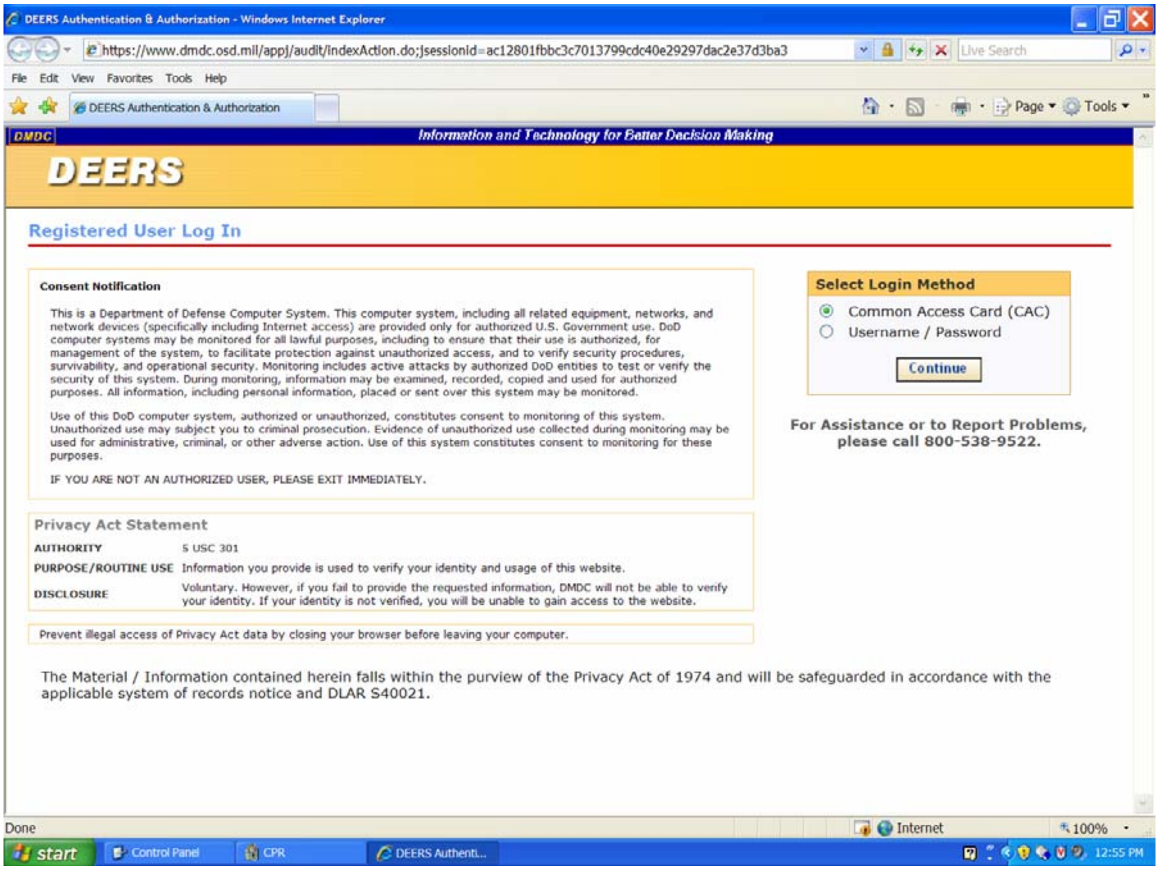
   Highlight both email certificates listed in the Certificates window and click *Remove* to remove the email certificates from the certificate store. Once the email certificates have been removed, click *Close* to close the Certificates window.

11. CTA REGISTRATION

1. CAC PKI certificates must be registered for CTAs prior to this function.
2. CTA registration forms are to be completed and maintained at the site level for all CTAs.

   These forms are: 1) Trusted Agent Security Manager (TASM) / CPR Trusted Agent (CTA) Registration/Revocation Form (Appendix C)
   2) CAC PIN Reset (CPR) User Qualifications Affidavit (Appendix D)
   3) TASM & CTA Acknowledge of Responsibilities (Appendix E)

3. To register a CTA, use the Online Security Web Application (https://www.dmdc.osd.mil/appj/audit/index.jsp).


DEERS Authentication & Authorization - Windows Internet Explorer
https://www.dmdc.osd.mil/appj/audit/indexAction.do;jsessionid=ac12801fbbc3c7013799cdc40e29297dac2e37d3ba3
Live Search
File Edit View Favorites Tools Help
DEERS Authentication & Authorization
Page Tools
DMDC
Information and Technology for Better Decision Making
DEERS
Done
Internet
100%
start
Control Panel
CPR
DEERS Authenti...
12:55 PM

Registered User Log In

Consent Notification

This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

IF YOU ARE NOT AN AUTHORIZED USER, PLEASE EXIT IMMEDIATELY.

Privacy Act Statement

AUTHORITY	5 USC 301
PURPOSE/ROUTINE USE	Information you provide is used to verify your identity and usage of this website.
DISCLOSURE	Voluntary. However, if you fail to provide the requested information, DMDC will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.

Prevent illegal access of Privacy Act data by closing your browser before leaving your computer.

Select Login Method

● Common Access Card (CAC)
○ Username / Password

Continue

For Assistance or to Report Problems, please call 800-538-9522.

The Material / Information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable system of records notice and DLAR S40021.

Online Security Web Application Logon Window

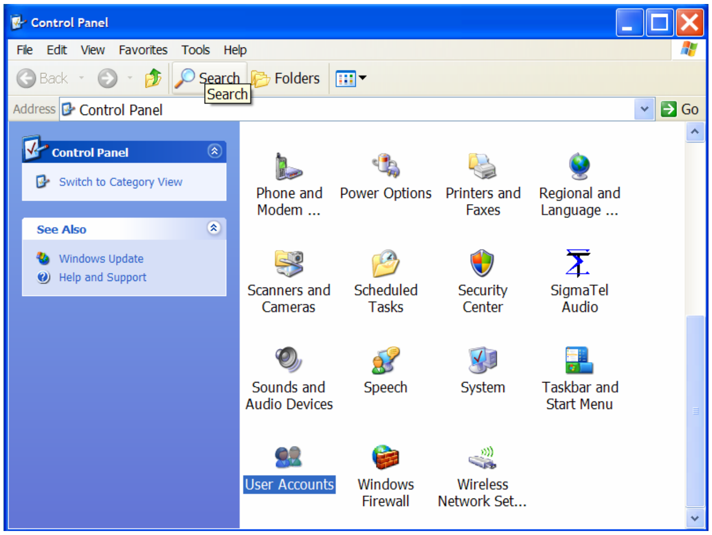
4. Refer to the Online Security Users Manual (http://pmo.cac.navy.mil/cpr/docs/Security_Online_Web_App_User_Manual.pdf) for specific instructions on how to administer users.
5. Once complete, it may take up to 48 hours for the user to be activated.

12. ADD A USER ACCOUNT TO THE WORKSTATION

Once a TASM or CTA is added to the CPR application, a user account will have to be created. Only a TASM can perform this task. The TASM will need Administrative or Power User rights to create this account.

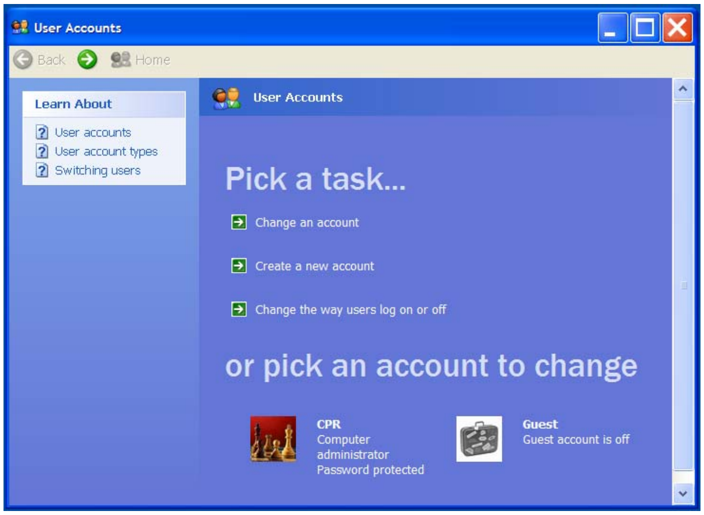
1. Open Control Panel by clicking *Start*, choose *Settings* from the menu then choose *Control Panel*.

2. Double-click the *Users Accounts* icon:



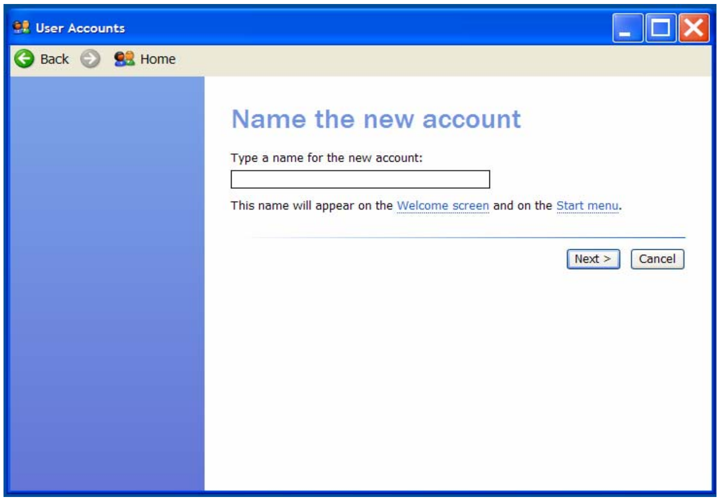
Control Panel Window

3. Select *Create a new account*:



User Accounts Window

4. Provide a name for the new account, then hit *Next*:



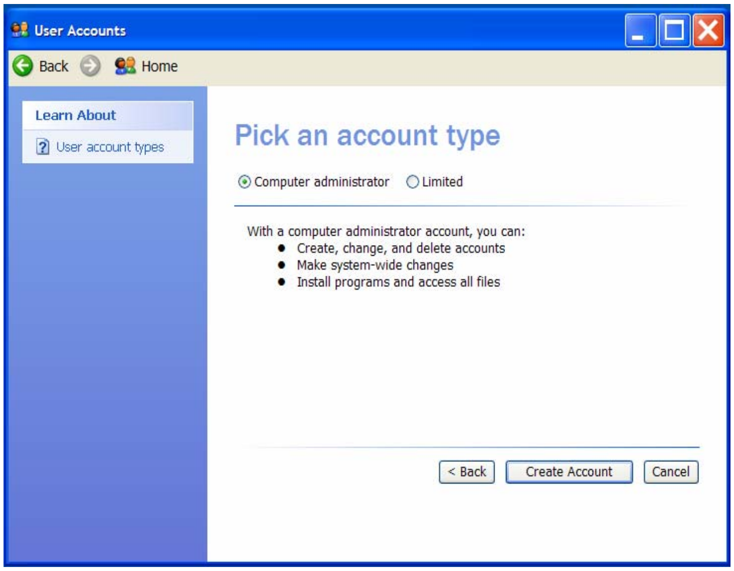
Name the new account

Type a name for the new account:

This name will appear on the Welcome screen and on the Start menu.

User Accounts Window

5. Select an account type. TASMs should be assigned an administrator role and CTA's should be assigned a limited role:



Pick an account type

● Computer administrator ○ Limited

With a computer administrator account, you can:

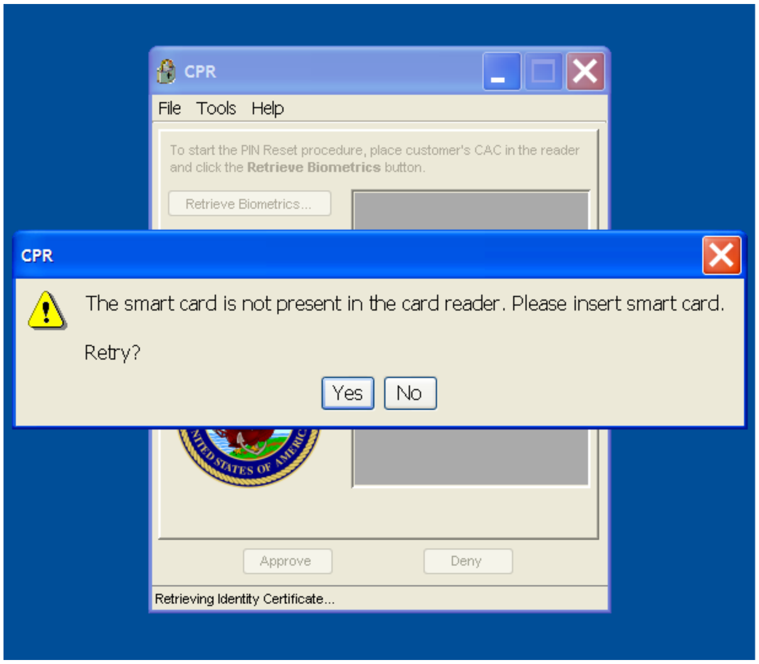
- Create, change, and delete accounts
- Make system-wide changes
- Install programs and access all files

User Accounts Window

13. APPLICATION LOGON

1. If you are not already logged on to the CPR workstation, logon by entering *Username* and *Password*.

2. Insert ***CAC*** into the CTA (ActivCard) Card Reader. Logon to the CPR application by double-clicking the *CPR* icon located on the desktop.



CPR

File Tools Help

To start the PIN Reset procedure, place customer's CAC in the reader and click the **Retrieve Biometrics** button.

Retrieve Biometrics...

CPR

The smart card is not present in the card reader. Please insert smart card.

Retry?

Yes No

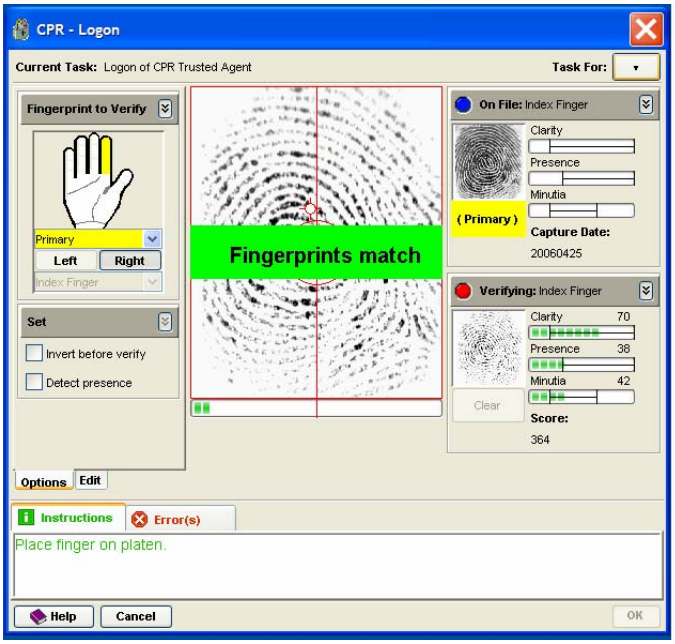
Approve Deny

Retrieving Identity Certificate...

Note: If the CAC is not present, the above message will appear. Insert the CAC into the card reader and click ***ok*** to continue.

3. Enter your *CAC PIN* when prompted then click *OK*.

4. *Provide a live scan fingerprint by placing your right index finger on the fingerprint scanner*. A green verification banner will display once a successful fingerprint match has been made. The CPR application will perform up to 3 fingerprint-matching attempts before timing out.



CPR - Logon

Current Task: Logon of CPR Trusted Agent

Task For:

Fingerprint to Verify

Primary

Left Right

Index Finger

Set

□ Invert before verify

□ Detect presence

Options Edit

Fingerprints match

On File: Index Finger

Clarity

Presence

Minutia

(Primary)

Capture Date: 20060425

Verifying: Index Finger

Clarity 70

Presence 38

Minutia 42

Clear

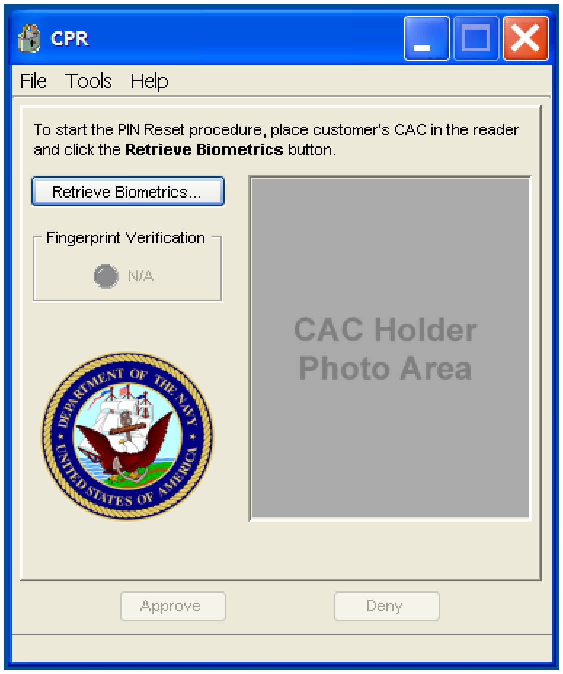
Score: 364

Instructions Error(s)

Place finger on platen.

Help Cancel OK

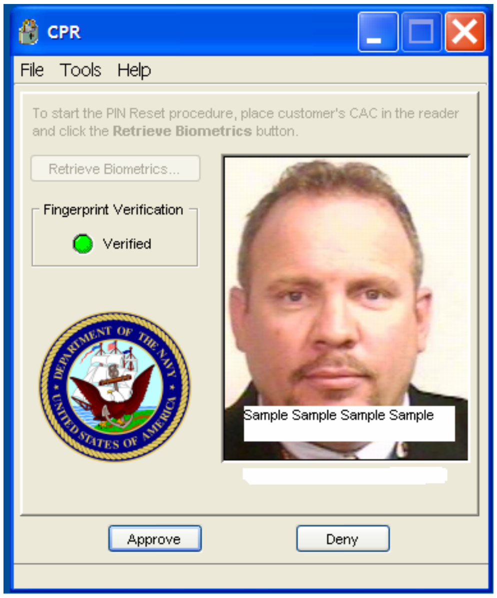
5. Once the fingerprint is verified, the *CPR* console will display:


To start the PIN Reset procedure, place customer's CAC in the reader and click the **Retrieve Biometrics** button.

CPR Console

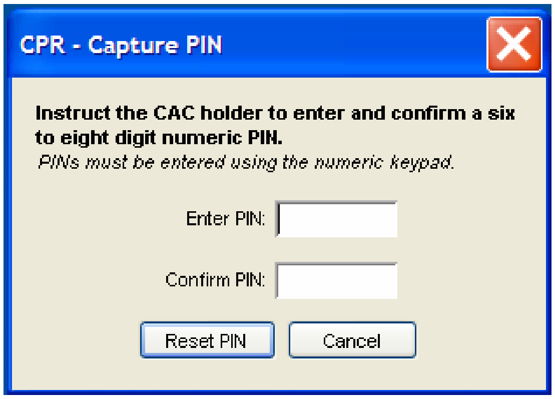
14. RE-SETTING A CUSTOMER'S PIN

1. Once the TASM/CTA has logged in to the application he/she can begin re-setting PINs
2. The CAC holder needing a PIN reset should insert the CAC into the SCR331 card reader.
3. Click the *Retrieve Biometrics* button on the CPR console window
4. The CAC holder will need to provide a live scan fingerprint by placing their right index finger on the fingerprint scanner
5. A green banner will display over the fingerprint indicating a successful fingerprint match. If the fingerprint is successfully matched, the CAC holder's photograph will then download from DEERS.


To start the PIN Reset procedure, place customer's CAC in the reader and click the **Retrieve Biometrics** button.

CAC Holder Digital Photo Display

6. A red light indicates that the fingerprint capture did not pass verification. The CPR application will perform up to three fingerprint-matching attempts before timing-out.
7. Verify the downloaded photograph to the CAC holder and click OK. **If photograph verification cannot be performed, the CAC holder must report to the RAPIDS issuance facility to reset the PIN.**
8. The CPR application will prompt the CAC holder to enter the new PIN twice. The CAC holder should hit enter after each PIN. **The new PIN can only be entered from the Numeric Keypad.** Click *OK* once the PIN has been entered twice.



CPR - Capture PIN

Instruct the CAC holder to enter and confirm a six to eight digit numeric PIN.
PINs must be entered using the numeric keypad.

Enter PIN:

Confirm PIN:

15. TECHNICAL ASSISTANCE

15.1. Troubleshooting Procedures

Before contacting the CPR help desk, follow these troubleshooting procedures:

a. Verify that the CPR workstation is correctly powered up. If operating under battery power, ensure the battery has been adequately charged prior to use.

b. Ensure that all peripherals are properly connected.

c. Ensure that Internet connectivity is operational and configured correctly for the workstation (Consult the TASM or Network Administrator, as necessary).

d. If logging on or authenticating to CPR is the problem, check that you are using the correct card reader and that it is attached. Contact the TASM for troubleshooting assistance and to double-check the workstation configuration. If the TASM can successfully log on and authenticate to the CPR, the problem may be a registration issue.

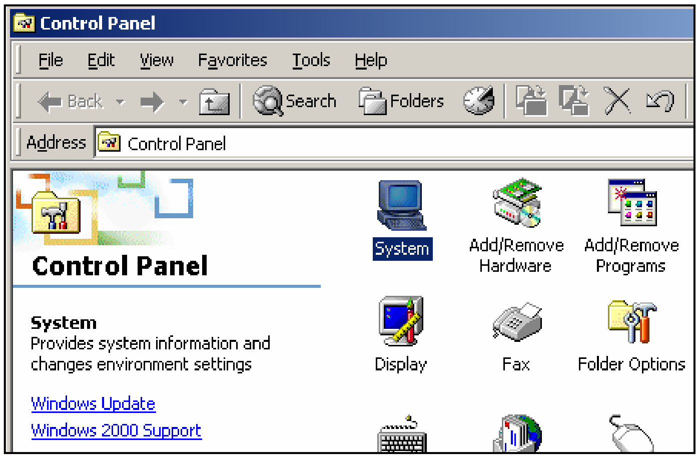
e. If all local troubleshooting efforts have been exhausted, contact the CPR help desk for assistance. Make sure to identify all efforts that have been attempted, and have the following information available:

- POC, email address and telephone number
- Site I.D. number
- Description of the problem

If it is determined through troubleshooting efforts that the workstation or any of the peripherals are defective, the CPR Project Manager will coordinate replacement.

Equipment Verification

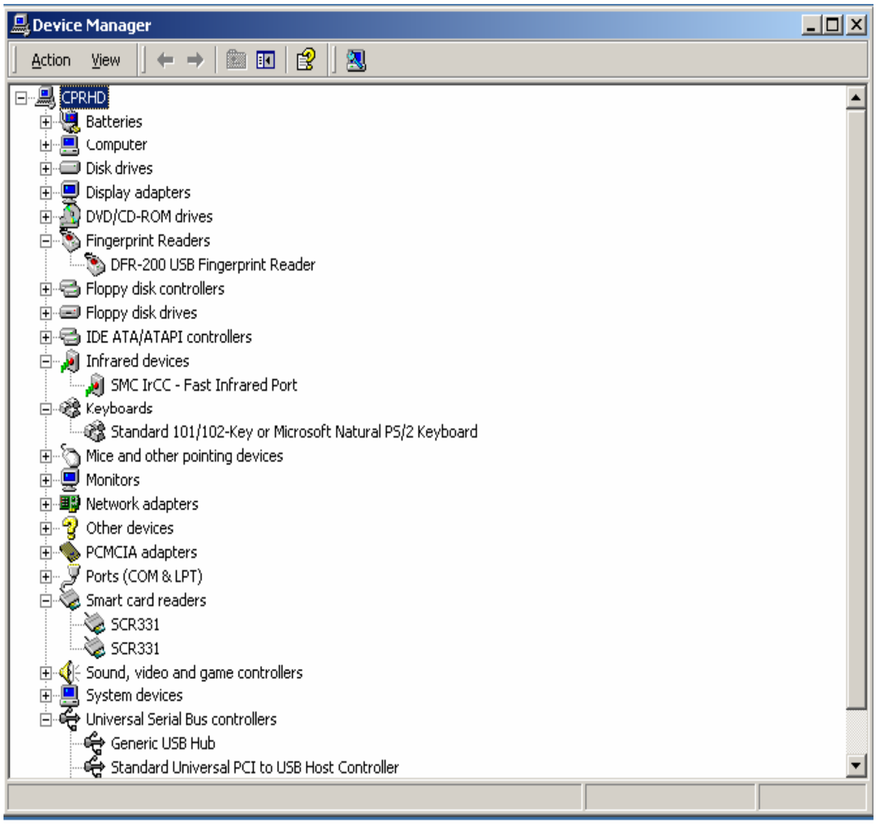
1. If unable to use one or more of the peripheral devices, check the Peripheral configuration by choosing the *System* icon from the *Control Panel*.



System
Provides system information and changes environment settings

Control Panel Window

2. If there is a configuration error with one of the devices, a question mark will appear before the device name.



```
CPRHD
  Batteries
  Computer
  Disk drives
  Display adapters
  DVD/CD-ROM drives
  Fingerprint Readers
    DFR-200 USB Fingerprint Reader
  Floppy disk controllers
  Floppy disk drives
  IDE ATA/ATAPI controllers
  Infrared devices
    SMC IrCC - Fast Infrared Port
  Keyboards
    Standard 101/102-Key or Microsoft Natural PS/2 Keyboard
  Mice and other pointing devices
  Monitors
  Network adapters
  Other devices
  PCMCIA adapters
  Ports (COM & LPT)
  Smart card readers
    SCR331
    SCR331
  Sound, video and game controllers
  System devices
  Universal Serial Bus controllers
    Generic USB Hub
    Standard Universal PCI to USB Host Controller
```

Device Manager Window

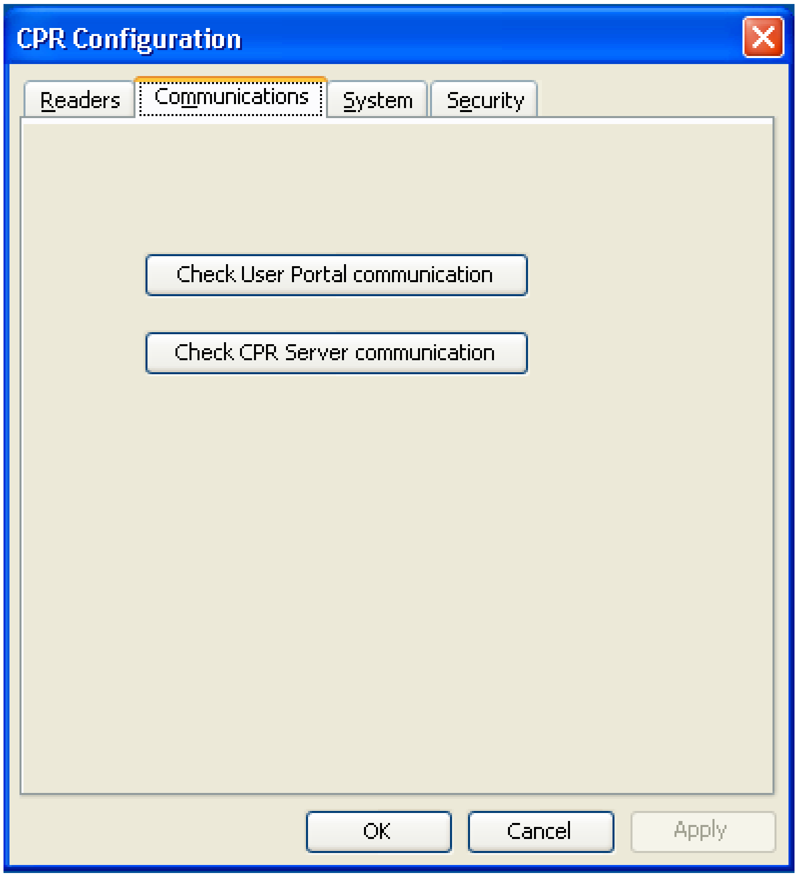
3. If the Device Manager indicates an error with one or more of the peripheral devices, check the connections and reboot the workstation.

4. In order to logon to the CPR application there must be no firewall obstructing communications and port 443 must be open. Check with local administrator to make sure these requirements are being met.

5. If you are unable to logon to the workstation, make sure that you are entering the provided password. Once you have logged on to the workstation for the first time, you will be prompted to change your password. This will be your new password for successive logons.

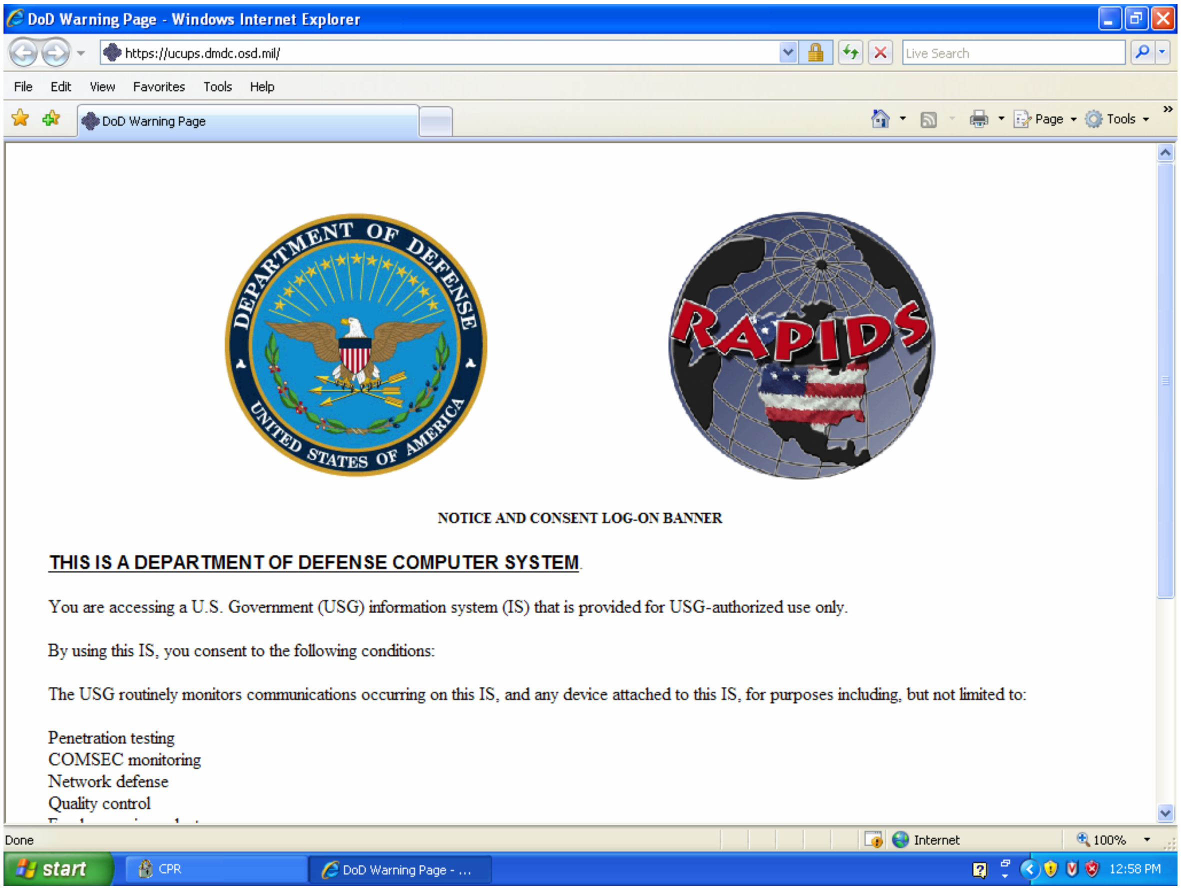
Communications test with DEERS/RAPIDS.

1. To test communications with DEERS/RAPIDS, click the *Tools* button on the CPR Console. The CPR Configuration Console displays. Click the *Check User Portal communication* button.



CPR Configuration Console Window

2. Windows Internet Explorer will display the following page if the communications between the workstation and DEERS/RAPIDS are functioning properly.



NOTICE AND CONSENT LOG-ON BANNER

THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM.

You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only.

By using this IS, you consent to the following conditions:

The USG routinely monitors communications occurring on this IS, and any device attached to this IS, for purposes including, but not limited to:

Penetration testing
COMSEC monitoring
Network defense
Quality control

DEERS/RAPIDS DOD Warning Page

15.1.1 Web Based Information

DMDC publishes policies, procedures, known solutions, and tips in the form of Frequently Asked Questions (FAQs), engineering-based solutions, and information from the DMDC knowledge base. When possible, users should consult the DMDC website (www.dmdc.osd.mil) for potential solutions prior to initiating trouble calls. The CAC PMO website (http://pmo.cac.navy.mil) publishes CPR policies, procedures and training.

15.2. Help Desk Support

TASMs and CTAs who are experiencing any difficulty with the CPR process should contact the CNIC Support Center or the CPR Project Manager. This includes workstation configuration and malfunctions, information regarding the CPR process and capability, training, and other difficulties. Help desk personnel will document and log all calls in the Trouble Report. If they are unable to provide problem resolution within 8 hours DMDC help desk support will be requested.

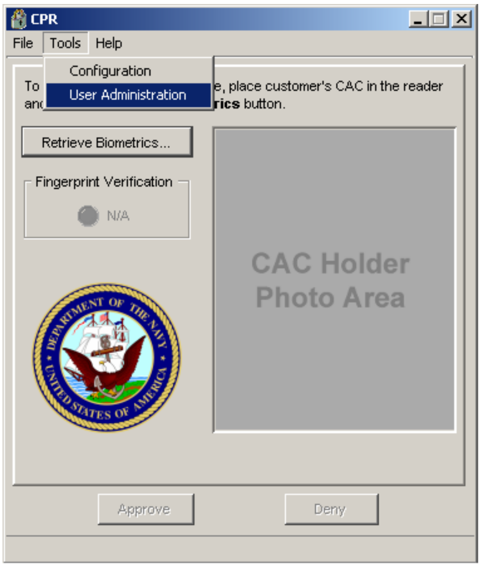
CNIC Support Center: (866)264-4255 / CPR Project Manager: (850)452-7895

15.2.1 CPR-MS Information Availability

Although primarily a management tool for the CPR Project Manager during CPR initial fielding efforts, additional capability may be added in subsequent releases to CPR-MS to allow the TASMs to review pertinent CPR information. This informational source will require authentication via CAC PKI certificates and allows these individuals to run CPR statistic queries for their respective areas of control. CAC PMO will notify sites when this capability becomes available.

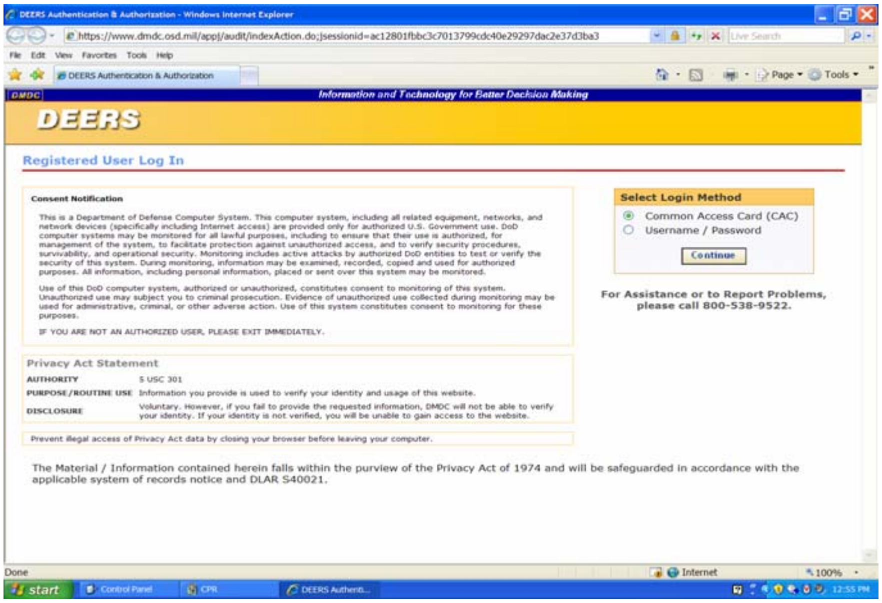
16. USER INFORMATION UPDATES

1. To administer user accounts, select *User Administration* from the *Tools* menu on the CPR Console:



CPR Console Window Tools Menu

2. Internet Explorer will start and the portal will display:


DEERS Authentication & Authorization - Windows Internet Explorer
https://www.dmdc.osd.mil/appj/audit/indexAction.do;jsessionid=ac12801fbbc3c7013799cdc40e29297dac2e37d3ba3
Live Search
File Edit View Favorites Tools Help
DEERS Authentication & Authorization
Page
Tools
DMDC
Information and Technology for Better Decision Making
DEERS
Registered User Log In

Consent Notification

This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.

IF YOU ARE NOT AN AUTHORIZED USER, PLEASE EXIT IMMEDIATELY.

Privacy Act Statement

AUTHORITY	5 USC 301
PURPOSE/ROUTINE USE	Information you provide is used to verify your identity and usage of this website.
DISCLOSURE	Voluntary. However, if you fail to provide the requested information, DMDC will not be able to verify your identity. If your identity is not verified, you will be unable to gain access to the website.

Prevent illegal access of Privacy Act data by closing your browser before leaving your computer.

Select Login Method

● Common Access Card (CAC)
○ Username / Password

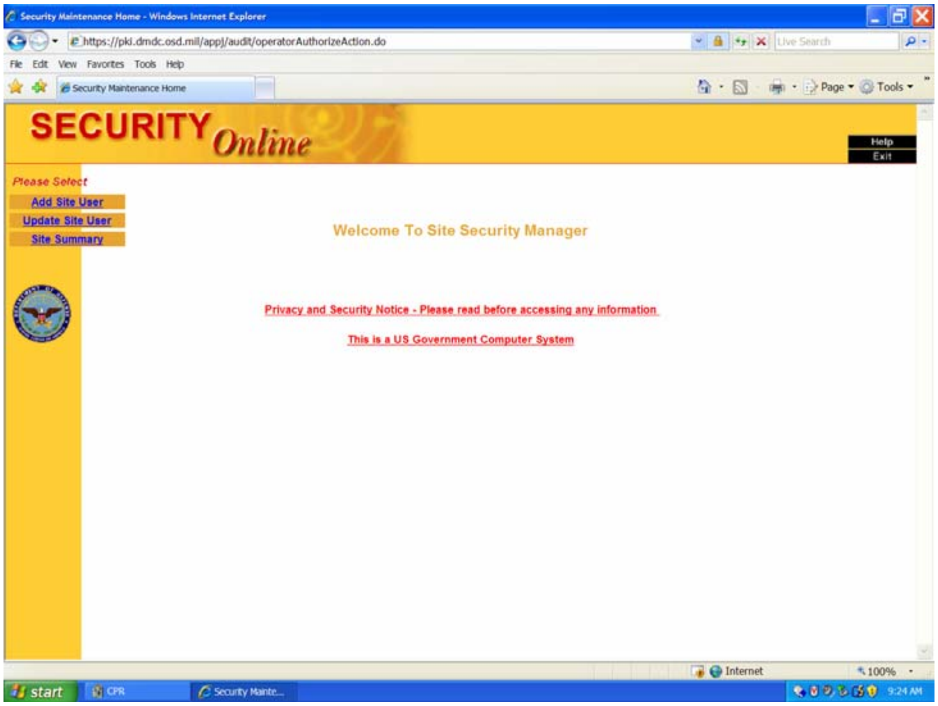
Continue

For Assistance or to Report Problems, please call 800-538-9522.

The Material / Information contained herein falls within the purview of the Privacy Act of 1974 and will be safeguarded in accordance with the applicable system of records notice and DLAR S40021.

Online Security Web Application Logon Window

3. Select the Common Access Card (CAC) Logon method.
4. Upon successful logon, the Site Security Manager page will display:


Security Maintenance Home - Windows Internet Explorer
https://pki.dmdc.osd.mil/appj/audit/operatorAuthorizeAction.do
File Edit View Favorites Tools Help
Security Maintenance Home
SECURITY Online
Help
Exit
Please Select
Add Site User
Update Site User
Site Summary
Internet
100%
start
CPR
Security Mainte...
9:24 AM

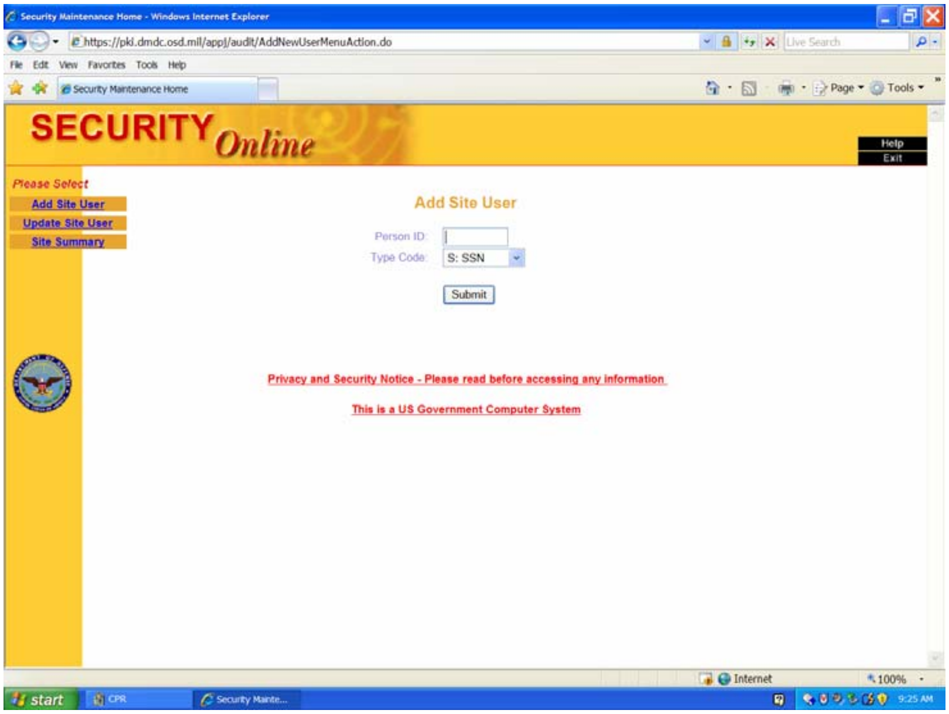
Welcome To Site Security Manager

Privacy and Security Notice - Please read before accessing any information

This is a US Government Computer System

Site Security Manager Window

5. Select the Add Site User link to add a user to your site:


Security Maintenance Home - Windows Internet Explorer
https://pki.dmdc.osd.mil/appj/audit/AddNewUserMenuAction.do
File Edit View Favorites Tools Help
Security Maintenance Home
SECURITY Online
Help
Exit
Please Select
Add Site User
Update Site User
Site Summary
Submit
Internet
100%
start
CPR
Security Mainte...
9:25 AM

Add Site User

Person ID:

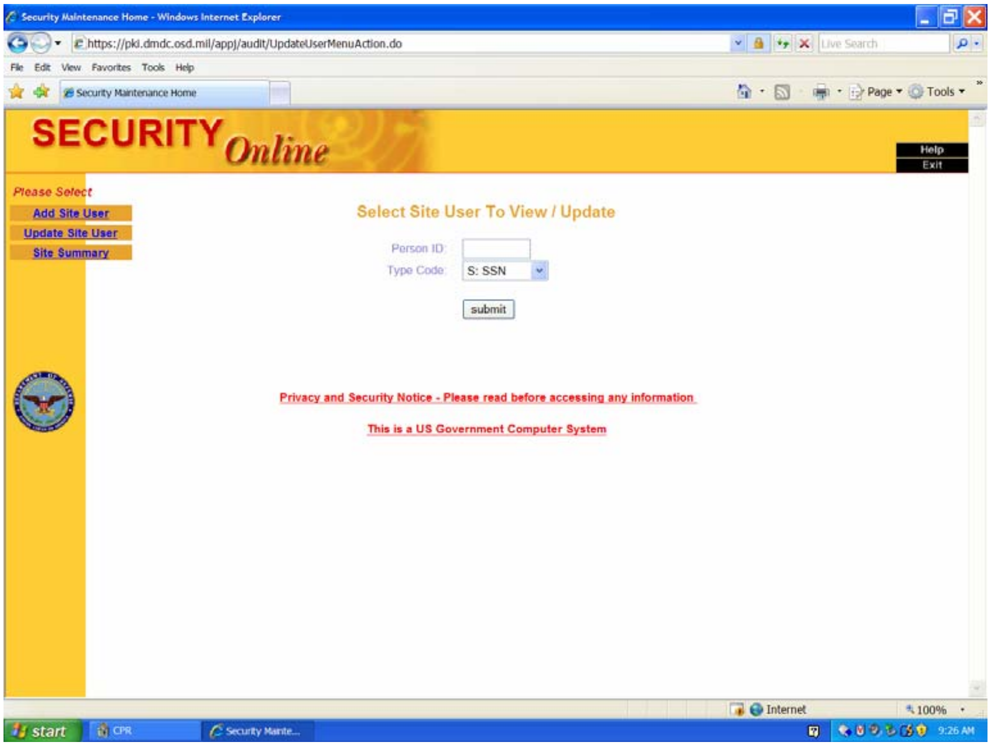
Type Code: S: SSN

Privacy and Security Notice - Please read before accessing any information

This is a US Government Computer System

Add a User Window using Site Security Manager

6. Select the Update Site User to View/Update a User's information:


Security Maintenance Home - Windows Internet Explorer
https://pki.dmdc.osd.mil/appj/audit/UpdateUserMenuAction.do
SECURITY Online
Help
Exit
Please Select
Add Site User
Update Site User
Site Summary
submit
Privacy and Security Notice - Please read before accessing any information
This is a US Government Computer System

Select Site User To View / Update

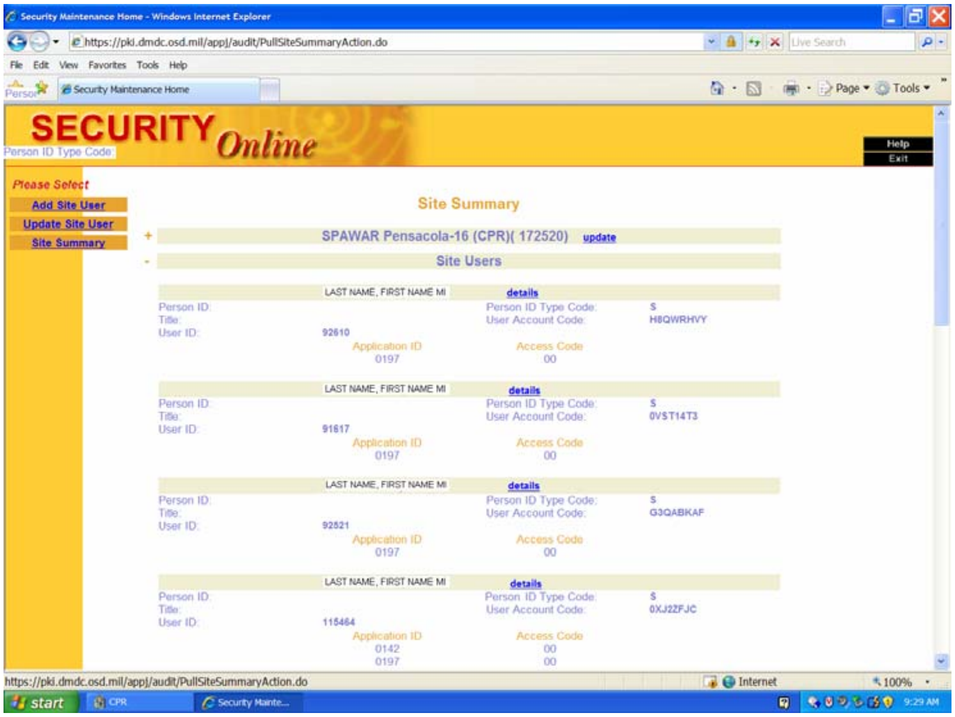
Person ID:

Type Code: S: SSN

Select Site User Window

17. CPR SITE ROSTER VIEWING

1. Select the Site Summary to view all of the Users assigned to your Site ID:


Security Maintenance Home - Windows Internet Explorer
https://pki.dmdc.osd.mil/appj/audit/PullSiteSummaryAction.do
SECURITY Online
Help
Exit
Please Select
Add Site User
Update Site User
Site Summary
update
details

Site Summary

SPAWAR Pensacola-16 (CPR)(172520)

Site Users

LAST NAME, FIRST NAME MI
Person ID: | Person ID Type Code: S
Title: | User Account Code: H8QWRHVY
User ID: 92610
Application ID 0197 | Access Code 00

LAST NAME, FIRST NAME MI
Person ID: | Person ID Type Code: S
Title: | User Account Code: 0VST14T3
User ID: 91617
Application ID 0197 | Access Code 00

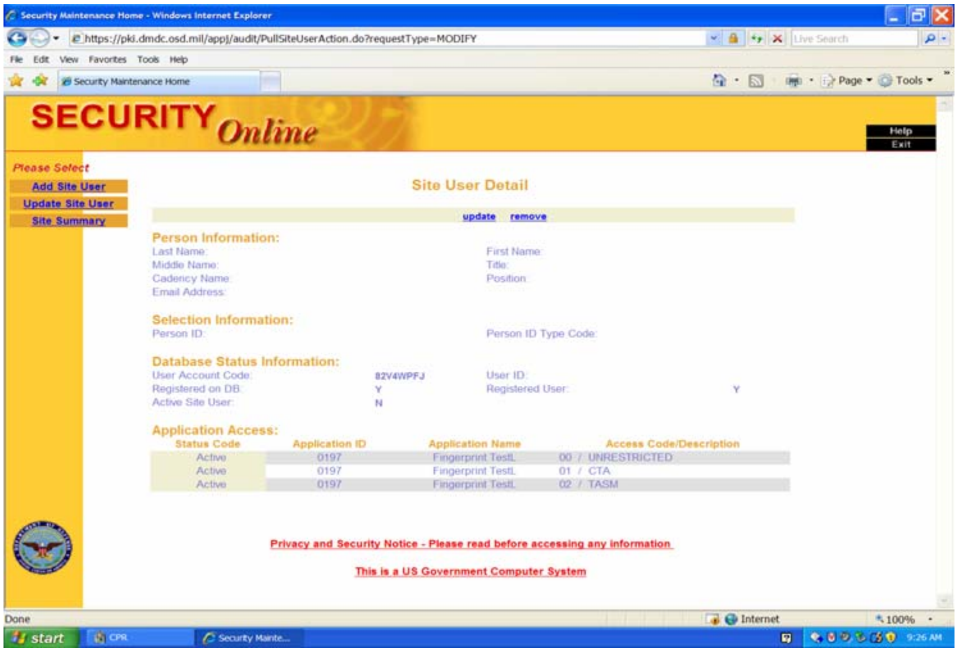
LAST NAME, FIRST NAME MI
Person ID: | Person ID Type Code: S
Title: | User Account Code: G3QABKAF
User ID: 92521
Application ID 0197 | Access Code 00

LAST NAME, FIRST NAME MI
Person ID: | Person ID Type Code: S
Title: | User Account Code: 0XJ2ZFJC
User ID: 115464
Application ID 0142 | Access Code 00
Application ID 0197 | Access Code 00

Site Security Manager - Site Summary View

18. USER REVOCATION

1. To remove a user from the CPR application, click *Update Site User*. This will display the User's information. Click *Remove* to delete the User's record. You will be prompted to confirm the deletion.


Security Maintenance Home - Windows Internet Explorer
https://pki.dmdc.osd.mil/appj/audit/PullSiteUserAction.do?requestType=MODIFY
File Edit View Favorites Tools Help
Security Maintenance Home
Page Tools
SECURITY Online
Help
Exit
Please Select
Add Site User
Update Site User
Site Summary
update remove
Privacy and Security Notice - Please read before accessing any information
This is a US Government Computer System
Done
Internet
100%
start
CPR
Security Mainte...
9:26 AM

Site User Detail

Person Information:
Last Name:
Middle Name:
Cadency Name:
Email Address:
First Name:
Title:
Position:

Selection Information:
Person ID:
Person ID Type Code:

Database Status Information:
User Account Code: 82V4WPFJ
Registered on DB: Y
Active Site User: N
User ID:
Registered User: Y

Application Access:

Status Code	Application ID	Application Name	Access Code/Description
Active	0197	Fingerprint TestL	00 / UNRESTRICTED
Active	0197	Fingerprint TestL	01 / CTA
Active	0197	Fingerprint TestL	02 / TASM

Site Security Manager – Site User Detail

19. AUDIT FILE REQUESTS

19.1. Reporting Requirements

At the direction of CPR Project Manager, TASMs must periodically transmit audit files created on the CPR workstation for sampling and measurement purposes.

19.2. Protection of Audit Files

All audit files must be protected from unauthorized viewing and tampering while residing on the CPR workstation during downloading and in transit. For this reason, files may only be viewed and manipulated by TASMs who are considered administrators of the CPR workstation. Additionally, files must be sent to CAC PMO (when requested) via digitally signed email.

19.3. Request for Audit Files

Request for audit files will be approved by the CPR Project Manager only. Audit files may only be requested by:

- TASMs
- DMDC officials (for troubleshooting or incident investigations)
- Law enforcement officials (for official investigations)

In each case, the requesting official must provide proof of identity and written justification for the file request. Proof of identity may be in the form of a valid government identification card or digitally signed email. Additionally, personnel may need to provide proof of purpose (i.e., warrant, official orders, etc.).

19.4. Frequency of Submission

There will be no regular interval for TASMs to submit audit files. Sampling of CPR workstation audit files will be done on a random basis, using Site IDs determined randomly by the CAC PMO and the DMDC engineering staff. Additionally, audit file transmissions may be requested whenever an anomaly is found within data received by the CPR Project Manager from DMDC.

20. AUDIT FILE RETRIEVAL

1. Double-click the *My Computer* icon on the Desktop then double-click the *Local Disk* ***(C:)*** icon. The audit files are located in the *C:\Program Files\CPR\logs\stats* folder. Copy the file *cpr_statslog4j.txt* to a diskette or USB data drive.

2. Right-click the *cpr_audit* file and choose *Send To*. Select your destination from the list.

3. Audit files should be sent to the CPR Project Manager via digitally signed and encrypted email.

21. POINTS OF CONTACT

CNIC, CAC Program Management Office
SPAWARSYSCEN Pensacola Office
Pensacola, FL 32508
CPR Project Office
(850) 452-7895
DSN 922-7895

Navy CPR Help Desk: (888) 264-4255

APPENDIX A. ACRONYMS AND ABBREVIATIONS

CAC	Common Access Card
CAC PMO	Common Access Card Program Management Office
CBT	Computer Based Training
COTS	Commercial, Off the Shelf
CPR	CAC Personal Identification Number Reset
CPR-DS	CPR DEERS Service
CPR-MS	CPR Management Service
CPR-PS	CPR Portal Service
CPR-WS	CPR Workstation
CTA	CPR Trusted Agent
CNI	Commander, Navy Installations
DEERS	Defense Enrollment Eligibility Reporting System
DMDC	Defense Manpower Data Center
DoD	Department of Defense
DoN	Department of the Navy
FAQs	Frequently Asked Questions
ID	Identification
PDR	Person Data Repository
PSD	Personnel Support Detachment
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Product Manager
POC	Point of Contact
RAPIDS	Real-time Automated Personnel Identification System
SNT	Sign-on Table
SOP	Standard Operating Procedures
SSAA	System Security Authorization Agreement
TASM	Trusted Agent Security Manager
UCMJ	Uniformed Code of Military Justice
USN	United States Navy
VO	Verifying Official

Appendix B. Request for Site-ID Registration

CPR Site Identification Registration Request

From: CAC Program Management Office, CPR Project Manager Date:

To: DEERS Security Team
DEERS/RAPIDS Operations Division
1555 Wilson Boulevard Suite 609
Arlington, Virginia 22209-2593 FAX (703) 578-5198

Subject: **Request for CAC PIN Reset (CPR) Site-ID: Registration** □ **Removal** □

Section I

Requesting Command:

Point of Contact Last Name: First Name:

Telephone: ( ) - DSN: -

Email address: @

Site Address 1:

Site Address 2:

City: State: Zip Code: Country:

Service/Organization: _____ Navy

Command POC:

Last Name: First Name:

Telephone: ( ) - DSN -

Email address: @

Section II: (To be completed by CAC PMO)

Approved by: Date Approved:

Section III: (To be completed by DEERS Security Office)

Approved by: Date Approved:

Appendix C. Request for TASM Registration/Revocation

CPR Trusted Agent Security Manager

Registration/Revocation Request

From: CAC Program Management Office, CPR Project Manager **Date**:

To: DEERS Security Team
DEERS/RAPIDS Operations Division
1555 Wilson Boulevard Suite 609
Arlington, Virginia 22209-2593

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 133 and E.O. 9397

PRINCIPAL PURPOSE(S): Collection of social security numbers and other personal identifiers is used to ensure positive identification of individuals in order to successfully register them as CPR users.

ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use as follows: The "Blanket Routine Uses" set forth at the beginning of OSD's compilation of systems of records notices apply to this system. The Federal and State agencies and private entities, as necessary, on matters relating to securing information during the conduct of official business, utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government facilities, computer systems networks, and controlled areas.

DISCLOSURE: Voluntary; however, failure to provide this information will result in failure to register an individual as a CPR user.

Section I

TASM Name: ____

Select one: **Primary TASM**____________ **Alternate TASM**____________

Social Security Number: ________ ______________

Telephone: _____________________________ **DSN:**____________________

Email address: ____

Command: ____

Address Line 1:____

Address Line 2____

City: _____________________ **State:** ______ **Zip Code:** _______

Action (select one): **Registration** ____________ **Revocation**______________

Approved/requested by: ________________________**Title:**_______________________

Telephone: ________________________ **DSN:** _______________________

Email address: ____

Section II: (To be completed by CPR Project Manager)

Approved by: **Date Approved:**

Section III: (To be completed by the DEERS Security Team)

Approved by: **Date Approved:**

Appendix D. CPR USER Qualifications Affidavit

Subject: CAC PIN Reset (CPR) User Qualifications Affidavit

To: CAC Program Management Office, CPR Project Manager

The individual named below been nominated as

( ) Trusted Agent Security Manager (TASM) ( ) CAC Pin Reset Trusted Agent (CTA)

I certify that by use of interviews or other means, I have confirmed that the named individual meets the following qualifications. The nominated individual:

- Is a Common Access Card (CAC) holder
- Is a United States citizen
- Has not been convicted of a felony offense, been knowingly denied a security clearance, or had a security clearance revoked
- Has had a National Agency Check (NAC) background investigation completed
- Is a DoD uniformed service member, DoD civilian, or contractor
- Is capable of sending and receiving digitally signed and encrypted email
- Is trustworthy
- Is knowledgeable of U.S. Navy property accountability procedures
- Has a minimum of six months retainability
- Has a working knowledge of the CPR system and the site to which they are assigned

CPR User Information

Name: ____
(Print)

Command: ____

Email address: ____________________ **Telephone:** ____________________

Requestor Information

Name: ____
(Print)

Signature: ____

Command: ____________________ **Title:** ____________________

Email address: ____________________ **Telephone:** ____________________

Appendix E. TASM & CTA Acknowledgement of Responsibilities Form

TASM & CTA
Acknowledgement of Responsibilities Form

____

(Printed name)

has been authorized to receive access to the DEERS system to support your operations as a Trusted Agent Security Manager (TASM) or CAC PIN Reset Trusted Agent (CTA). The information located on your Common Access Card will enable you to gain access to systems for the purpose of CAC PIN Reset. These systems are government property and may only be used for official purposes.

Acknowledgement of Responsibilities: I acknowledge that I have received U.S. Navy approved training to act as a user of the CAC PIN Reset (CPR) system. I understand that as a CPR User, I will be responsible for the following:

- I will conduct TASM or CTA operations in accordance with the stipulations of an approved Navy CPR Business Process Policy Statement and Standard Operating Procedures.
- For TASMs Only: I will ensure that other TASMs and CTAs are trained and capable of continuing CPR capability for the site in my absence.
- I will use my Common Access Card, and the privileges it conveys, only for official purposes.
- I will follow all specified physical security requirements with regards to the protection of the CPR workstation.
- I will not disclose my PIN to anyone or leave it where it might be observed.
- I will never leave the CPR workstation unattended with my CAC inserted into the reader.
- I will report the compromise of my workstation password, or PIN to the appropriate authorities.
- I will report any suspected misuse (attempted or actual) of the CPR workstation to the appropriate authorities.
- I will follow all approved procedures to verify the identity of CAC holders requesting PIN reset.
- For those CAC holders whose identity cannot be verified or authenticated, I will direct them to the nearest DEERS/Rapids CAC Issuance Facility. Additionally, if attempted compromise is suspected, I will contact the CAC Issuance Facility separately to alert them to the situation.
- I will keep a copy of this Acknowledgement of Responsibilities form in compliance with current practices.

Liability: A CPR User will have no claim against the DOD arising from use of the TASM or CTA privileges. In no event will the DOD be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any erroneous PIN reset procedure.

Governing Law: the laws of the United States of America shall govern the CPR process and equipment.

Acceptance: I understand that once I obtain and use my CPR user privileges that I have accepted the authority of the laws and regulations governing those privileges.

Name: ____ **Date:** ______________________

Signature

Command: _______________________________________ **Site ID #:** __________________

Local Commander or Security Official: I have personally witnessed the TASM/CTA apply the signature above, and personally verified the identity of the person receiving the CAC PIN Reset User credentials.

Name: ____ **Date:** ______________________

Signature

Title: _____________________________________ **Command**: ________________________________

Appendix F. CTA Acknowledgement of Responsibilities Form

CPR Trusted Agent (CTA)
Acknowledgement of Responsibilities Form

____
(Printed name)

is authorized to receive access to the DEERS system to support your operations as a CAC PIN Reset Trusted Agent (CTA). The information located on your Common Access Card will enable you to gain access to systems for the purpose of CAC PIN Reset. These systems are government property and may only be used for official purposes.

Acknowledgement of Responsibilities: I acknowledge that I have received U.S. Navy approved training to act as a user of the CAC PIN Reset (CPR) system. I understand that as a CPR User, I will be responsible for the following:

- I will conduct CTA operations in accordance with the stipulations of an approved Navy CPR Business Process Policy Statement and Standard Operating Procedures.
- I will use my Common Access Card, and the privileges it conveys, only for official purposes.
- I will follow all specified physical security requirements with regards to the protection of the CPR workstation.
- I will not disclose my PIN to anyone or leave it where it might be observed.
- I will never leave the CPR workstation unattended with my CAC inserted into the reader.
- I will report the compromise of my workstation password, or PIN to the appropriate authorities.
- I will report any suspected misuse (attempted or actual) of the CPR workstation to the appropriate authorities.
- I will follow all approved procedures to verify the identity of CAC holders requesting PIN reset.
- For those CAC holders whose identity cannot be verified or authenticated, I will direct them to the nearest DEERS/Rapids CAC Issuance Facility. Additionally, if attempted compromise is suspected, I will contact the CAC Issuance Facility separately to alert them to the situation.
- I will keep a copy of this Acknowledgement of Responsibilities form in compliance with current practices.

Liability: A CPR User will have no claim against the DOD arising from use of the CTA privileges. In no event will the DOD be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any erroneous PIN reset procedure.

Governing Law: the laws of the United States of America shall govern the CPR process and equipment.

Acceptance: I understand that once I obtain and use my CPR user privileges that I have accepted the authority of the laws and regulations governing those privileges.

Name: ____ **Date:** ______________________
Signature

Site ID: ______________ **Phone:** __________________________ **DSN:** ___________________

Email address: ____

Command: ____

Local Commander or Security Official: I have personally witnessed the CTA apply the signature above, and personally verified the identity of the person receiving the CAC PIN Reset User credentials.

Name: ____ **Date:** ______________________
Signature

Title: ____________________________________ **Command:** ________________________________

Appendix G. Site Survey Worksheet

The information on this worksheet is required to configure CAC PIN Reset workstations for a specific CPR site.

Site Survey Worksheet

Command: ____

Requested by: ____

Telephone #:   commercial__________________________   DSN_____________

Shipping address for the CPR workstation: ____________________________

____

City: ___________________ State: ____________ Zip Code: ______

- -

If your site uses Static IP assignment as opposed to DHCP, please fill out remainder of Worksheet.

IP Address Range for CPR workstations (as assigned by the local system administrator)

-     -   -   Through   -   -   -

Internet gateway IP address (as determined by the local system administrator)

-     -   -

Additional security requirements for access to the Internet from your site (consult your local system administrator and explain):

Appendix H. TASM Information Change Request

CPR Trusted Agent Security Manager Change Request

From: CAC, PMO, CPR Project Manager Date: ________________________

To: DEERS Security Team
DEERS/RAPIDS Operations Division
1555 Wilson Boulevard Suite 609
Arlington, Virginia 22209-2593

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C. 133 and E.O. 9397
PRINCIPAL PURPOSE(S): Collection of social security numbers and other personal identifiers is used to ensure positive identification of individuals in order to successfully register them as CPR users.
ROUTINE USES: In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use as follows: The "Blanket Routine Uses" set forth at the beginning of OSD's compilation of systems of records notices apply to this system. The Federal and State agencies, private entities, as necessary, on matters relating to securing information during the conduct of official business, utilization review, professional quality assurance, program integrity, civil and criminal litigation, and access to Federal government facilities, computer systems networks and controlled areas.

DISCLOSURE: Voluntary; however, failure to provide this information will result in failure to register an individual as a CPR user.

Section I

Site ID: _______________

Command: ____

TASM Name: ____

Social Security Number: _______________________ Designation: Primary □ Alternate □

Telephone: (   ) - _____________ DSN: _________________________

Email address: ____

Site Address:

____

____

City:___________________________ State: ________ Zip Code: ________ Country: _______

Section II: (To be completed CAC PMO)

Approved by: ________________________________ Date Approved: ______________

Section III: (To be completed by the DEERS Security Team)

Approved by: ________________________________ Date Approved: ______________